Pergamon

Appl. Math. Lett. Vol. 8, No. 5, pp. 81–86, 1995

0893-9659/95 $9.50 + 0.00

0893-9659(95)00071-2

An Updated Table of Rate $1/p$ Binary Quasi-Cyclic Codes

T. A. GULLIVER
Department of Systems and Computer Engineering, Carleton University
1125 Colonel By Drive, Ottawa, Ontario, Canada K1S 5B6

V. K. BHARGAVA
Department of Electrical and Computer Engineering, University of Victoria
P.O. Box 3055, Victoria, BC, Canada V8W 3P6

(Received January 1995; accepted February 1995)

Abstract—In this paper, an updated table of maximum minimum distances for rate $1/p$ binary quasi-cyclic (QC) codes is presented. Many of the new codes given attain the bounds in the table by Brouwer and Verhoeff and the expanded table maintained by Brouwer, and fourteen of these codes improve the bounds. The generator polynomials of the new QC codes which provide table improvements are given. These codes were found using integer linear programming and a heuristic combinatorial optimization algorithm.

Keywords—Quasi-cyclic codes, Bounds on binary linear codes.

1. INTRODUCTION

Quasi-cyclic (QC) codes are a generalization of cyclic codes whereby a cyclic shift of a codeword by p positions results in another codeword. This class of codes is known to contain many good binary linear codes [1–4]. Here, a *good* code is defined as one which has the maximum known minimum distance for a given n and k; i.e., it attains or exceeds the known lower bound on the minimum distance. A *best* code is defined as one which achieves the maximum possible minimum distance for a given class of linear codes. An *optimal* code is one which achieves the maximum possible minimum distance for a linear code.

Many QC codes can be characterized in terms of $m \times m$ circulant matrices, so that the block-length is a multiple of m, $n = mp$. In this case, the code has rate $1/p$ and an $m \times mp$ generator matrix of the form

$$G = [C_0,\ C_1,\ C_2,\ C_3, \ldots,\ C_{p-1}], \tag{1}$$

where C_i is an $m \times m$ binary circulant matrix defined as

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\ c_{m-2} & c_{m-1} & c_0 & \cdots & c_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}. \tag{2}$$

The algebra of circulant $m \times m$ matrices over GF(2) is isomorphic to the algebra of polynomials in the ring $f[x]/x^m - 1$ if C is mapped onto the polynomial, $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m-1} x^{m-1}$ [5]. The polynomial representation is used here for convenience.

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada.

The algorithm used to find good codes is based on the approach in [2] which employs integer linear programming and heuristic combinatorial optimization techniques. Nonexhaustive methods are used where an exhaustive search via linear programming is intractable. Although the resulting codes are not guaranteed to be the best possible, codes which meet or exceed the lower bounds on the minimum distance can still be obtained. Those which attain the upper bound are necessarily optimal. The above structure of the QC codes was exploited to accelerate the search.

The first table of maximum minimum distances for rate $1/p$ binary QC codes was given in [2]. Since that time, many new codes have been found which improve this table. The updated maximum minimum distances are compiled in Table 1. A superscript ^{o} denotes a best possible QC code. This was determined either by integer linear programming, or meeting a known upper bound. The fourteen new codes which improve the bounds in [6,7] on the maximum minimum distance of binary linear codes are listed in Table 2. The minimum distances from [6,7] are given for comparison, and are denoted as d_{br}. The generator polynomials, $c_i(x)$, are given in octal, with the least significant coefficient on the left; i.e., 365_8 corresponds to $x^7+x^5+x^3+x^2+x+1$. As an example, consider the (225,9) code with $d_{\min} = 110$ with generator polynomials listed in Table 2. The generator matrix for this code is given in Table 3. The weight distribution is as follows.

Weight	Count
0	1
110	324
112	117
126	60
128	9
144	1

Numerous agreements with the bounds in [6,7] were also found. These results provide further evidence that the class of QC codes will yield many more good codes.

REFERENCES

1. T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2, *IEEE Trans. Inf. Theory* **IT-20**, 679 (1974).
2. T.A. Gulliver and V.K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes, *IEEE Trans. Inf. Theory* **IT-37**, 552–555 (May 1991).
3. T.A. Gulliver and V.K. Bhargava, Nine good rate $(m-1)/pm$ quasi-cyclic codes, *IEEE Trans. Inf. Theory* **IT-38**, 1366–1369 (July 1992).
4. T.A. Gulliver and V.K. Bhargava, Twelve good rate $(m-r)/pm$ quasi-cyclic codes, *IEEE Trans. Inf. Theory* **IT-39** (September 1993).
5. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, (1977).
6. A.E. Brouwer and T. Verhoeff, An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inf. Theory* **IT-39**, 662–677 (March 1993).
7. A.E. Brouwer, Table of minimum-distance bounds for linear codes, Eindhoven University of Technology, Eindhoven, The Netherlands, (1993).
8. H.C.A. van Tilborg, On quasi-cyclic codes with rate $1/m$, *IEEE Trans. Inf. Theory* **IT-24**, 628–629 (September 1978).
9. C. Zhi, Private Communication, (January 1993).

APPENDIX

Table 1. Maximum minimum distances for (pm, m) quasi cyclic codes.

	p										
m	3	4	5	6	7	8	9	10	11	12	13
3	$4^{=o}$	$6^{=o}$	$8^{=o}$	$10^{=o}$	$12^{=od_{12}}$	$13^{=o}$	$15^{=o}$	$16^{=o}$	$18^{=o}$	$20^{=o}$	$22^{=o}$
4	$6^{=o}$	$8^{=o}$	$10^{=o}$	$12^{=od_4}$	$14^{=o}$	$16^{=od_4}$	$18^{=o}$	$20^{=o}$	22^{o}	$24^{=od_4}$	26^{o}
5	$7^{=o}$	$9^{=o}$	$12^{=od_4}$	$15^{=o}$	$16^{=o}$	$20^{=o}$	$22^{=o}$	$24^{=od_4}$	27^{o}	$30^{=o}$	$32^{=o}$
6	$8^{=od_4}$	$10^{=o}$	$14^{=o}$	$16^{=o}$	$20^{=od_4}$	$24^{=od_8}$	$26^{=o}$	29^{-o}	$32^{=od_4}$	34^{-o}	$38^{=o}$
7	$8^{=o1}$	$12^{=o1d_4}$	$16^{=o1}$	$19^{=o1}$	22^{-o1}	$26^{=o1}$	$31^{=o1}$	$33^{=o1}$	$36^{=o1}$	$40^{=o1}$	$44^{=o1}$
8	$8^{=o1}$	12^{-o1}	$16^{=o1}$	20^{o1}	$24^{=o1}$	28^{-o1}	$32^{=o1d_4}$	$37^{=o1}$	40^{-o1}	$46^{=o1}$	$48^{=o1}$
9	$10^{=o}$	$14^{=o}$	$18^{=o}$	$23^{=o}$	$28^{=o}$	$32^{=od_4}$	$36^{=o}$	$40^{=}$	46^{eo}	50^{e}	55^{e}
10	10^{-o}	$16^{=o}$	$20^{=o}$	24^{o}	30^{-}	$34^{=}$	$40^{=d_4}$	$44^{=}$	49^{e}	54	$60^{=}$
11	11^{-o}	$16^{=o}$	21^{-o}	$28^{=od_4}$	$32^{=}$	$39^{=}$	43^{e}	$48^{=}$	53^{-}	59^{e}	$64^{=}$
12	$12^{=o}$	$17^{=o}$	$24^{=o}$	$28^{=d_4}$	$34^{=}$	$40^{=}$	46^{e}	$52^{=d_4}$	56^{-}	62	$68^{=}$
13	$12^{=o}$	$19^{=o}$	$25^{=}$	30	$36^{=}$	43^{-}	$48^{=}$	54	60	66	72
14	$13^{=o}$	$20^{=o}$	$26^{=}$	$32^{=}$	38	44	50	57	64^{d_4}	70	76
15	$14^{=o}$	20	26	34	40	$48^{=}$	54	60	68	74	80
16	14^{o}	21	28	$36^{=d_4}$	42	50	$57^{=}$	$64^{=}$	72	80^{d_4}	86
17	$16^{=o}$	23	29	$36^{=}$	44	$52^{=}$	$60^{=}$	66	74	82	90
18	$16^{=o}$	$24^{=2}$	30^{-}	38	46	54	$62^{=}$	70	78	86	94
19	$16^{=}$	$24^{=}$	$32^{=2}$	40^{-2}	48	56^{-}	64	72	80	88	96
20	$16^{=}$	$24^{=2}$	32^{-2}	41^{2}	50	58	68				
21	$18^{=2}$	$26^{=2}$	$34^{=2}$	43^{2}	52	60	70	$80^{=}$	88	98	108
22	$18^{=}$	$28^{=2}$	$36^{=2}$	44	54	$64^{=}$	68	79	88	98	108
23	18	28^{-2}									
24	18	27^{-}	36	47	57	68	78	93^{e}			
25	19^{-}	$28^{=}$	38								
26	$20^{=}$	$30^{=}$	40	$50^{=}$							

(continued on next page)

Notes:
- n^{o} a best QC code.
- $n^{=}$ equals the best minimum distance in [7].
- n^{-} one less than the best minimum distance in [7].
- n^{e} provides the best minimum distance in [7].
- n^{1} constructed by van Tilborg [8].
- n^{2} constructed by Zhi [9].
- n^{d_z} the code exists with weights divisible by z.

Table 1. (continued)

	p											
m	14	15	16	17	18	19	20	21	22	23	24	25
3	$24^{=od_{24}}$	$25^{=o}$	$27^{=o}$	$28^{=o}$	$30^{=o}$	$32^{=o}$	$34^{=o}$	$36^{=o}$	$37^{=o}$	$39^{=o}$	$40^{=o}$	$42^{=o}$
4	28^{od_4}	$32^{=od_{32}}$	$33^{=o}$	$36^{=od_4}$	$38^{=o}$	$40^{=o}$	$42^{=o}$	$44^{=o}$	$46^{=o}$	$48^{=o}$	$50^{=o}$	$52^{=o}$
5	$35^{=o}$	37^{-o}	$40^{=o}$	42^{-o}	45^{-o}	$48^{=o}$	$50^{=o}$	52^{-o}	$56^{=o}$	$58^{=o}$	60^{-o}	$64^{=o}$
6	40^{-o}	$44^{=o}$	$48^{=o}$	$50^{=o}$	53^{-o}	$56^{=o}$	$60^{=o}$	63^{-o}	$65^{=o}$	$68^{=o}$	$72^{=o}$	74^{-}
7	$48^{=o1}$	$52^{=o1}$	$56^{=o1}$	$59^{=o1}$	$63^{=o}$	$64^{=o}$	$68^{=o}$	$72^{=o}$	$76^{=o}$	$80^{=o}$	$83^{=o}$	$87^{=o}$
8	$54^{=o1}$	$57^{=o1}$	$64^{=od_{64}}$	$66^{=o}$	$70^{=o}$	74^{eo}	$78^{=o}$	$81^{=}$	$86^{=o}$	$90^{=o}$	$96^{=o}$	$98^{=o}$
9	$59^{=}$	$64^{=o}$	68^{e}	$72^{=}$	77^{e}	81^{e}	87^{e}	92^{eo}	$96^{=o}$	100^{eod4}	$104^{=}$	110^{eo}
10	$64^{=}$	$68^{=}$	74^{e}	80^{ed_8}	$84^{=}$	94^{e}	$98^{=}$	$104^{=}$	109	$114^{=}$	118	
11	69^{e}	75^{e}	$80^{=}$	84	90^{-}	$96^{=}$			116			
12	$74^{=}$	80^{d_4}	86	92^{d_4}	96^{d_4}							
13	78	84	92	98	104							
14	84	89	96	102	108							
15	88	94	102	108	116							
16	94	103	113	118	125							
17	98	105										
18	102											
19	104	116	124	132	140							
20												
21	118	127										
22	118	127	139									
23												
24												
25												
26												

Notes:
- n^{o} a best QC code.
- $n^{=}$ equals the best minimum distance in [7].
- n^{-} one less than the best minimum distance in [7].
- n^{e} provides the best minimum distance in [7].
- n^{1} constructed by van Tilborg [8].
- n^{2} constructed by Zhi [9].
- n^{d_z} the code exists with weights divisible by z.

Table 2. Rate m/pm QC codes which improve the bounds on the maximum possible minimum distance for a binary linear code.

code	$d_{\min}$	new d_{br}	$c_i(x)$
(152, 8)	74	74	1, 5, 7, 13, 15, 23, 25, 27, 31, 37, 45, 57, 65, 67, 73, 75, 127, 133, 177
(144, 9)	68	68–69	127, 57, 133, 15, 23, 13, 137, 277, 53, 63, 73, 253, 135, 257, 43, 25
(162, 9)	77	77–78	165, 1, 17, 25, 133, 67, 75, 43, 137, 153, 253, 7, 357, 117, 147, 31, 47, 23
(171, 9)	81	81–83	173, 377, 177, 71, 75, 37, 25, 67, 273, 337, 165, 31, 127, 3, 125, 133, 35, 157, 357
(180, 9)	87	87–88	57, 51, 31, 53, 137, 127, 153, 133, 147, 253, 177, 277, 21, 25, 55, 43, 23, 13, 27, 75
(189, 9)	92	92	253, 21, 31, 165, 117, 173, 47, 25, 13, 57, 23, 1, 377, 267, 175, 7, 65, 133, 273, 147, 17
(207, 9)	100	100	31, 75, 25, 57, 23, 47, 1, 55, 125, 3, 155, 137, 51, 73, 377, 167, 153, 7, 175, 3, 127, 157, 273
(225, 9)	110	110	63, 137, 35, 1, 125, 153, 277, 377, 51, 7, 177, 147, 75, 337, 53, 273, 117, 113, 357, 57, 37, 267, 67, 155, 165
(243, 9)	118	118–120	175, 177, 63, 357, 257, 253, 25, 73, 267, 113, 135, 377, 123, 337, 75, 37, 273, 51, 155, 153, 45, 35, 5, 65, 127, 133, 147
(170, 10)	80	80–82	11, 157, 135, 225, 77, 115, 43, 573, 55, 253, 527, 53, 567, 165, 233, 111, 107
(200, 10)	94	94–96	777, 57, 333, 677, 337, 163, 667, 355, 335, 567, 315, 123, 51, 47, 757, 17, 77, 25, 61, 247
(132, 11)	59	59–62	211, 13, 373, 61, 527, 477, 237, 251, 637, 117, 23, 345
(154, 11)	69	69–72	445, 473, 217, 33, 57, 243, 773, 227, 263, 335, 463, 105, 131, 465
(165, 11)	75	75–78	7, 71, 351, 1677, 525, 737, 213, 327, 121, 523, 657, 5, 455, 13, 635

Table 3. Generator matrix for the optimal (225,10) $d_{\min} = 110$ QC code.

000110011	001011111	000011101	000000001	001010101	001101011	010111111	011111111	000101001	000000111	001111111	001100111	000111101	011011111
100011001	100101111	100001110	100000000	100101010	100110101	101011111	101111111	100010100	100000011	100111111	100110011	100011110	101101111
110001100	110010111	010000111	010000000	010010101	110011010	110101111	110111111	010001010	110000001	110011111	110011001	010001111	110110111
011000110	111001011	101000011	001000000	101001010	011001101	111010111	111011111	001000101	111000000	111001111	111001100	101000111	111011011
001100011	111100101	110100001	000100000	010100101	101100110	111101011	111101111	100100010	011100000	111100111	011100110	110100011	111101101
100110001	111110010	111010000	000010000	101010010	010110011	111110101	111110111	010010001	001110000	111110011	001110011	111010001	111110110
110011000	011111001	011101000	000001000	010101001	101011001	111111010	111111011	101001000	000111000	111111001	100111001	111101000	011111011
011001100	101111100	001110100	000000100	101010100	110101100	011111101	111111101	010100100	000011100	111111100	110011100	011110100	101111101
001100110	010111110	000111010	000000010	010101010	011010110	101111110	111111110	001010010	000001110	011111110	011001110	001111010	110111110

000101011	010111011	001001111	001001011	011101111	000101111	000011111	010110111	000110111	001101101	001110101
100010101	101011101	100100111	100100101	101110111	100010111	100001111	101011011	100011011	100110110	100111010
110001010	110101110	110010011	110010010	110111011	110001011	110000111	110101101	110001101	010011011	010011101
011000101	011010111	111001001	011001001	111011101	111000101	111000011	111010110	111000110	101001101	101001110
... 101100010	101101011	111100100	101100100	111101110	111100010	111100001	011101011	011100011	110100110	010100111
010110001	110110101	011110010	010110010	011110111	011110001	111110000	101110101	101110001	011010011	101010011
101011000	111011010	001111001	001011001	101111011	101111000	011111000	110111010	110111000	101101001	110101001
010101100	011101101	100111100	100101100	110111101	010111100	001111100	011011101	011011100	110110100	111010100
001010110	101110110	010011110	010010110	111011110	001011110	000111110	101101110	001101110	011011010	011101010